Remarks

Status of application

Claims 1-70 were examined and stand rejected in view of prior art. The claims have been amended to further clarify Applicant's invention. Reexamination and reconsideration are respectfully requested.

The invention

System and methodology are described for protecting new computers by applying a preconfigured security update policy. In one embodiment, for example, a method of the present invention is described for controlling connections to a new computer upon its initial deployment, the method comprises steps of: before deployment of the new computer, imaging the computer's storage to include a preconfigured security update policy for preventing Internet-borne infections occurring before the computer can obtain security-relevant updates; upon the initial deployment of the new computer, applying the preconfigured security update policy to establish at the computer a pre-access restricted zone of at least one preapproved host that the computer is restricted to connect to upon its initial deployment for obtaining current security-relevant updates, so that the computer is completely blocked from all other connectivity to the Internet until security-relevant updates have been completed; receiving a request for a connection from the computer to a particular host; based on the preconfigured security update policy, determining whether the particular host is within the restricted zone of at least one preapproved host; blocking the connection if the particular host is not within the restricted zone of at least one preapproved host; and once the computer has complied with the security update policy, lifting the restricted zone so that the computer is allowed to participate with general connectivity to the Internet.

Section 101 rejection

Claim 25 stands rejected under 35 U.S.C. 101 on the basis that the claimed invention is directed to non-statutory subject matter. The claim has been amended to remove "a downloadable set of processor-executable instructions" phraseology and replace it with a method step, thus clarifying that the claimed invention is directed to a

process or method.

Prior art rejections

A. Section 103 rejection: Freund and Fazal

Claims 1-4, 8-19, 22-29, 33-44, 47-52, 56-67 and 70 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Freund (US 5,987,611) in view of Fazal et al. (hereinafter Fazal) US 2005/0246767. The Examiner's rejection of claim 1 is representative:

> Freund discloses a method for controlling connections to a computer, the method comprising:
>
> applying a pre-configured security policy that establishes a restricted zone of at least one pre-approved host that the computer may connect to, so that the computer is not allowed to participate with general connectivity to the internet until security- relevant updates have been completed; (col. 3, line 5-67; col. 14, lines 14-23; col. 15, lines 26- 33; col. 16, lines 1-3; a client-side filter that is controlled by the centralized authority .. .the centralized authority has a way of enforcing non-compliance)
>
> receiving a request for a connection from the computer to a particular host; (col. 4, lines 51-55; col. 5, lines 44-45; the system can monitor TCPIIP activities .. .if a particular client has access rights to the Internet ... trapping a request for Internet access from a client computer)
>
> based on said pre-configured security policy, determining whether the particular host is within the restricted zone of at least one pre-approved host; (col. 4, lines 3-4; col. 5, lines 6-8; the centralized supervisor application is installed on a computer on the LAN that can be reached from all workstations that need access to the Internet)
>
> blocking all clients that have not been verified by the supervisor application; (col. 4, lines 51-55; col. 5,10-15 and lines 46-47; col 15, lines 26-col. 16, line 3; the system can monitor TCPIIP activities .. .if a

particular has access rights to the Internet ...determining whether the request for the Internet access would violate any of the rules transmitted to the particular client; the supervisor monitors whether a client has the filter application loaded and provides the filter application ...the supervisor application signals the firewall which client applications have been certified so that the firewall only grants Internet access to those clients)

blocking said connection if said particular host is not within the restricted zone of at least one pre-approved host; (col. 4, line 3-4; col. 5, lines 49-51; col. 28, lines 30-31; col. 19, lines 61-66; if the request for Internet access violates any of the rules ... denying the request for Internet access .. .if the supervisor detects any problem with the client, It notifies the firewall to disable Internet access for the client) and

once the computer has complied with the security update policy, lifting the restricted zone so that the computer is allowed to participate with general connectivity to the internet (col. 3, line 64-col. 4, line 4; col. 14, lines 14-23; col. 15, lines 26-33; col. 16, lines 1-3; a supervisor application that maintains the access rules for the client based filter and verifies the existence and proper operation of the client-based-filter application (installed at each client) ...and provides filter application with the rules for the specific user or workstation).

Freund does not explicitly disclose controlling connections to a computer upon its initial deployment of the computer. Fazal in analogous art, however, discloses controlling connections to a computer upon its initial deployment of the computer. (page 1, pp.8; page 3. pp. 34; page 4, pp. 43-52; 4, pp.41; only device that are found to be in compliant with a predefined corporate security policy may be allowed to access the network or network services; page 6, pp.69-71; when a new device attempts to connect to the network the server determines whether the new device fulfills corporate standards, if so the server enables access and if the new device is not up-to-date, the device is instructed to contact the update server). Therefore it would have been obvious to one ordinary skill in the

art at the time the invention was made to modify the method disclosed by Freund with Fazal in order to ensure the security features of connected devices are up-to-date and non-compliant devices have limited access, if any, thereby discovering the current state of connected devices and update device as early as possible in the timeline. (page 1, pp.6; Fazal)

The Examiner has adopted Applicant's own prior patent (Freund '611) as the cornerstone of his rejection. In Applicant's prior Amendment (08/06/2007), the claims were amended to prevent such an interpretation. Subsequent to Applicant's Appeal, the Examiner has now reopened prosecution by adding Fazal, Perkins, and Marchosky (in different combinations) to Applicant's own Freund '611, to fashion various Section 103 rejections. However as will be shown below, Applicant's invention may be distinguished on a variety of grounds.

At the outset Applicant of course concedes that the underlying endpoint security system (commercial product of ZoneAlarm®), which is the subject of the Freund '611 patent, is used as part of the embodiment of the present invention. To be sure there is (of necessity) overlap between Applicant's present invention and the endpoint security system (subject matter of the Freund '611 patent) that it uses. That said, a critical distinction exists between Applicant's present invention and the prior art (including in combination with Freund '611), as will now be described.

The original ZoneAlarm® Security Suite product (as well as all other security products, including Norton, McAfee, etc.) have no notion of a "pre-access restricted zone" specifically for a new machine (i.e., one that has never been connected to the Internet before). This "pre-access restricted zone" constitutes firewall and access rules that limit a new machine at the system level to only accessing specific sites (i.e., sites that the manufacture is aware of at the time that the image is built). Since the new machine operates in a restricted zone upon the initial deployment, the machine initially cannot be remotely accessed by another computer (e.g., a computer which is connected via a LAN or WAN). This restriction specifically addresses the "chicken and egg" problem faced with new machines -- that they can (and will) get infected immediately upon connection to the Internet due to out-of-date firewall and antivirus software, yet they cannot get up-

to-date firewall and antivirus software until they connect to the Internet. This is not merely a theoretical problem but a real-world problem that has led to significant costs and lost productivity due to infections of new computers. In particular, this chicken-and-egg problem to computer security for new machines is very insidious due to hacker probes, such as the MS-Blast worm, where an infection can occur simply by virtue of a machine connecting to the Internet (i.e., no user activity (e.g., web browsing) is required at all in order to pick up an infection).

Although Applicant believes that the previously pending claims distinguish over the art of record, Applicant has nevertheless redoubled efforts to clarify Applicant's invention by amending the claims further. For instance, claimed 1 now includes the following (shown in amended form):

> 1. (Currently amended) A method for controlling connections to a new computer upon its initial deployment, the method comprising:
>
> before deployment of the new computer, imaging the computer's storage to include a preconfigured security update policy for preventing Internet-borne infections occurring before the computer can obtain security-relevant updates;
>
> upon the initial deployment of the new computer, applying ~~a~~ said preconfigured security update policy to establish at the computer ~~that establishes~~ a pre-access restricted zone of at least one preapproved host that the computer ~~may~~ is restricted to connect to upon its initial deployment for obtaining current security-relevant updates, so that the computer is ~~not allowed to participate with general~~ completely blocked from all other connectivity to the Internet until security-relevant updates have been completed;

At this point in his rejection (i.e., as to the first claim limitation of claim 1), the Examiner points to Applicant's own Freund '611 for providing " a client-side filter that is controlled by the centralized authority .. .the centralized authority has a way of enforcing non-compliance." However, such falls far short of Applicant's amended claim limitation.

Specifically, the claim language sets forth at the new computer itself (i.e., without requiring a network enforcement mechanism, such as Fazal) a "pre-access restricted zone" comprising the host(s) (e.g., antivirus vendor update website) that the new computer is restricted to upon its initial deployment. Importantly, the new computer includes a fully self-contained enforcement mechanism to completely block all other connectivity until security-relevant updates have been obtained for the new computer.

The Examiner relies on Fazal for the proposition that it "discloses controlling connections to a computer upon its initial deployment of the computer." This reliance is misplaced. Fazal simply discusses connecting computers to a network (e.g., corporate network) that includes Fazal's network security system. There is no indication whatsoever from Fazal that such connection is the initial deployment of a new computer, as now required by Applicant's amended claims. More importantly, Applicant's amended claims require that the new computer itself in fact be imaged to include a preconfigured security update policy for preventing Internet-borne infections occurring before the new computer can obtain security-relevant updates. This "self contained" solution is a critical distinction -- one that solves the chicken-and-egg problem faced, which is faced daily by mobile computer users who connect to public (open) networks.

In order to best understand the distinction, it is helpful to review the environment that mobile computing devices now face. Consider the following from Applicant's specification ([0007-0008]):

> In traditional computing networks, a desktop computer largely remained in a fixed location and was physically connected to a single local network (e.g., via Ethernet). More recently, however, an increasingly large number of business and individual users are using portable computing devices, such as laptop computers, that are moved frequently and that connect into more than one network. For example, many users now have laptop computers that can be connected to networks at home, at work, and in numerous other locations. Many users also have home computers that are remotely connected to various organizations from time to time through the Internet. The number of computing devices, and the

number of networks that these devices connect to, has increased dramatically in recent years.

In addition, various different types of connections may be utilized to connect to these different networks. A dial-up modem may be used for remote access to an office network. Various types of wireless connectivity, including IEEE (Institute of Electrical and Electronics Engineers) 802.11 and Bluetooth, are also increasingly popular. **Wireless networks often have a large number of different users. Moreover, connection to these networks is often very easy, as connection does not require a physical link. Wireless and other types of networks are frequently provided in cafes, airports, convention centers, and other public locations to enable mobile computer users to connect to the Internet. Increasingly, users are also using the Internet to remotely connect to a number of different systems and networks. Thus, it is becoming more common for users to connect to a number of different networks from time to time through a number of different means.**

(Emphasis added.)

Fazal's approach to security stems from the traditional notion of a computing network (i.e., described in the first paragraph above), such as a corporate or "enterprise" network that computers are connected to. As described in the excerpt from Applicant's specification above, that traditional view does not represent today's mobile computing workforce. Thus, Applicant's approach to security is based on today's reality of a dynamic or ever-changing computing network, such as commonly faced by laptop users today. Simply put, today's mobile computing user cannot rely on a network-based approach to security (e.g., Fazal's approach) as "the network" itself is no longer a fixed or static corporate network but is, instead, whatever WiFi hub the user happens to be located by. Thus, in the current environment, "the network" often is a WiFi access point provided by a third party (e.g., café, airport, hotel, etc.) which may be under no particular duty to provide any sort of network-based security for the user.

With Applicant's approach, the newly deployed computer does not have to depend upon the network having any sort of security mechanism. With Applicant's approach it is assumed that the network will not have any sort of security mechanism to protect the computer, and thus the "newborn" computer must fend for itself in a manner akin to a newborn shark which is born fully equipped (with razor-sharp teeth so that it can fend for itself immediately upon birth). In fact, with Applicant's approach the network that the new computer first connects to may is frequently untrusted or in fact hostile, such as a public WiFi access point that is compromised. Fazal's network-centric approach to security management (which relies on a network under one's control to host his network-based security system) teaches, if anything, away from Applicant's device-centric approach.

Each new machine configured in accordance with Applicant's invention (e.g., receiving disk image configured as such) will be limited to only contacting a limited set of security-relevant sites (i.e., pre-access restricted zone). Importantly, all other attempted connections to the machine (i.e., from non-approved addresses) are refused during the pre- and peri-access stage. Only upon a given new computer completing updating of security subsystems will that computer allow any other connections to occur. This approach is fully self-contained within the four corners of the computer itself and does not rely on any network (or network-based security system) to monitor or enforce security compliance at the computer. The cited prior art does not provide such functionality (but instead teaches the opposite). Reading such features into the art at this juncture at best simply applies the hindsight benefit of Applicant's present invention. Quite simply, prior art versions of security software simply gave machines general connectivity to the Internet and provided firewall and antivirus protection with versions (and definition files) that were effectively guaranteed to be out-of-date by the time the machines reached consumer hands. Network-based approaches, such as Fazal, do not address this problem since "the network" is -- in today's mobile computing world -- typically a third party network (e.g., public WiFi) that is largely if not completely uncontrolled.

In view of the amendments to the claims and the remarks made above, it is respectfully submitted that the claims set forth a patentable advance over the art, and that

any rejection under Section 103 is overcome.

B. Section 103 rejection: Freund, Fazal, and Perkins

Claims 5-6, 30-31 and 53-54 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Freund (above) in view of Fazal et al. (above) and in view of Perkins et al. (US 2004/0187028 A1). Here, the Examiner repeats the rejection based on Freund and Fazal above, but adds Perkins for the contention that it teaches the claim limitation of "wherein said preconfigured security update policy operates to prevent the computer from being remotely accessed by another computer upon the initial deployment." The claims are believed to be allowable for at least the reasons cited above pertaining to the first Section 103 rejection. Perkins itself includes no teaching overcoming this deficiency.

Appellant's independent claims were previously amended to emphasize that a "security update policy" is applied during this restricted access stage, for limiting the computer's connectivity. This is computer-implemented logic intrinsic to the new computer (i.e., not requiring external supervisor computer or network-based security module) that has the specific additional effect of obliging or forcing the user to update his or her new computer before the general Internet connectivity is allowed. Importantly, the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed, even if the new computer is connected to a totally unprotected network. As none of the prior art systems (including Appellant's own' 611 patent) function in such a manner, it is respectfully submitted that those systems do not provide an adequate basis of prior art to teach or suggest Appellant's claimed invention, or render Appellant's invention obvious in view of the combination of Freund and Fazal with Perkins. Thus, the combined references do not form an adequate basis of rejection under Section 103.

C. Section 103 rejection: Freund, Fazal, and Aroya

Claims 7, 32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Freund (above) in view of Fazal et al. (above) and in view of Aroya (US 2004/0177274 A1). Here, the Examiner repeats the rejection based on Freund and Fazal above, but adds Aroya for the contention that it teaches the claim limitation pertaining to preventing the

computer from being infected by a malicious program delivered through an open port. The claims are believed to be allowable for at least the reasons cited above pertain to the first Section 103 rejection. Aroya itself includes no teaching overcoming this deficiency. Simply put, the prior art references when combined do not teach or suggest all the claim limitations, and thus do not form an adequate basis of rejection under Section 103.

D. Section 103 rejection: Freund, Fazal, and Marchosky

Claim 20 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Freund (US 5,987,611) in view of Fazal et al. (hereinafter Fazal) US 2005/0246767 in view of Marchosky (US 2004/0117215 A1). Here, the Examiner repeats the rejection based on Freund and Fazal above, but adds Marchosky for the contention that it teaches the claim limitation pertaining to providing a warning to the user and displaying a disclaimer to the user. The claims are believed to be allowable for at least the reasons cited above pertain to the first Section 103 rejection. Marchosky itself includes no teaching overcoming this deficiency. Again, the Examiner has formulated a combination of prior art references that do not teach or suggest all the claim limitations, and do not form an adequate basis of rejection under Section 103.

E. Section 102 rejection: Albert

Claims 1, 26 and 49 stand rejected under 35 U.S.C. 102(e) as being anticipated by Albert et al. (hereinafter Albert) US 2003/0177389. The Examiner's rejection of claim 1 is representative:

> Albert discloses a method for controlling connections to a computer upon its initial deployment, the method comprising:
>
> Upon the initial deployment, applying a pre-configured security policy that establishes a restricted zone of at least one pre-approved host that the computer may connect to, so that the computer is not allowed to participate with general connectivity to the internet until security- relevant updates have been completed; (figures 5A and 58; page 3., pp.24-25; page 5, pp. 50-51; page 9, pp. 80-83)

receiving a request for a connection from the computer to a particular host; (figures 5A and 58; page 3., pp.24-25; page 5, pp. 50-51; page 9, pp. 80-83) based on said pre-configured security policy, determining whether the particular host is within the restricted zone of at least one pre-approved host; (figures 5A and 58; page 3., pp.24-25; page 5, pp. 50-51; page 9, pp. 80-83)

blocking all clients that have not been verified by the supervisor application; (figures 5A and 58; page 3., pp.24-25; page 5, pp. 50-51; page 9, pp. 80-83)

blocking said connection if said particular host is not within the restricted zone of at least one pre-approved host; (figures 5A and 58; page 3., pp.24-25; page 5, pp. 50- 51; page 9, pp. 80-83) and

once the computer has complied with the security update policy, lifting the restricted zone so that the computer is allowed to participate with general connectivity to the internet (figures 5A and 58; page 3., pp.24-25; page 5, pp. 50-51; page 9, pp. 80- 83)

Here, the Examiner likens Applicant's invention to Applicant's own (i.e., assignee Check Point's own) Security Policy Arbitration invention (Albert '389).

The Albert '389 patent filing relates to the merging together or arbitrating different (particularly disparate) security policies. Albert enables multiple security policies to be effectively reconciled and merged as required from time to time -- that is, dynamically or on-the-fly -- so that the user's device has the security policies and settings appropriate for the then-current connection(s) -- at some period of time long after initial deployment has occurred. Here, Albert employs a flexible merged or arbitrated security policy that is generated and constantly regenerated by arbitrating setting of each of the active policies (i.e., ones pertinent for the current connections). In cases of conflicting rules, the policies are arbitrated by adopting the most restrictive (i.e., most secure) rule. Albert is fundamentally different from the claimed invention here.

Albert describes the merging of disparate security policies together but does not describe a self-contained (i.e., device-contained) enforcement mechanism for requiring a

new computer upon deployment to completely block all other connectivity until security-relevant updates have been obtained for it. In fact, the pre-access restricted zone policy would, upon initial deployment of the new computer, trump all other policies that may be available, so there isn't even any collection of competing policies to merge (in accordance with Albert). Instead, the security update policy would reign supreme -- restricting general Internet connectivity -- until such time as the required security update has been carried out. Once the required update has been completed, the restriction is lifted. Only after the restriction is lifted (i.e., after the present invention has completed its work) is the notion of merging various security policies (a la Albert) even relevant.

All told, Albert shares little in common with Applicant's present invention, other than being inventions by the same company (Check Point Technologies, Inc.) and thus (of course) in the same field of technology. There is no merging or arbitration of security policies with Applicant's approach. By the same token, Albert does not include any discussion pertaining to preconfiguration of new computers in a manner that would allow them to obtain security-relevant updates before being infected by an Internet-borne computer virus or other malware. Accordingly, it is respectfully submitted that the claims distinguish over Albert (particularly in view of clarifying amendments made herein) and that any rejection under Section 102 is overcome.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: October 24, 2008

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX